The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/13/2010

SUBJECT:
Vulnerabilities in SMB Client Could Allow Remote Code Execution (MS10-020)

OVERVIEW:
Five vulnerabilities have been discovered in Microsoft Server Message Block (SMB) Client that could allow for remote code execution or denial of service. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices. These vulnerabilities could be exploited if an attacker hosts a specially crafted SMB server that is designed to exploit these vulnerabilities and then convinces a user to initiate an SMB connection with the attacker. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user or cause a denial-of-service condition. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Windows 2000
Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Five vulnerabilities have been discovered in Microsoft Server Message Block (SMB) Client that could allow for the remote code execution or cause a denial of service condition. These vulnerabilities could be exploited if an attacker hosts a specially crafted SMB server that is designed to exploit these vulnerabilities and then convinces a user to initiate an SMB connection with the attacker. Additionally, an attacker on the local network could perform a man-in-the-middle attack to respond to a legitimate SMB request with a malformed SMB response.

SMB Client Incomplete Response Vulnerability
Microsoft SMB Client is vulnerable to a client incomplete response vulnerability that could allow for denial of service conditions. This vulnerability exists due to the way that the Microsoft SMB Client

implementation handles specially crafted SMB responses. An attempt to exploit this vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. This will cause the server to stop responding until it is manually restarted.

SMB Memory Allocation Vulnerability
Microsoft SMB Client is vulnerable to a memory allocation vulnerability which could allow for remote code execution. This vulnerability exists due to the way that the Microsoft SMB Client implementation allocates memory when parsing specially crafted SMB responses. An attempt to exploit this vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request.

SMB Client Transaction Vulnerability
Microsoft SMB Client is vulnerable to a client transaction vulnerability which could allow for remote code execution. This vulnerability exists due to the way that the Microsoft SMB Client implementation handles specially crafted SMB transaction responses. An attempt to exploit this vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request.

SMB Client Response Parsing Vulnerability
Microsoft SMB Client is vulnerable to a client response parsing vulnerability which could allow for remote code execution. This vulnerability exists due to the way that the Microsoft SMB Client implementation parses specially crafted SMB transaction responses. An attempt to exploit this vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request.

SMB Client Message Size Vulnerability
Microsoft SMB Client is vulnerable to a client message size vulnerability which could allow for remote code execution. This vulnerability exists due to the way that the Microsoft SMB Client implementation handles specially crafted SMB responses. An attempt to exploit this vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request.

Successful exploitation of the last four vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Implement egress and ingress filtering for TCP ports 139 and 445 at your network perimeter.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/Ms10-020.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0269
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0270
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0476

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0477

Security Focus:
http://www.securityfocus.com/bid/36989
http://www.securityfocus.com/bid/39340
http://www.securityfocus.com/bid/39339
http://www.securityfocus.com/bid/39336
http://www.securityfocus.com/bid/39312